

Required security and sovereignty capabilities

The RFP should require:

- **Data and jurisdiction controls:** Approved locations for production data, metadata, telemetry, logs, backups and disaster-recovery copies; disclosure of corporate ownership, subprocessors, remote-support locations and government-access procedures.
- **Identity and privileged access:** Federated SSO, phishing-resistant MFA, least privilege, workload identities, privileged-access management, just-in-time administration, separation of duties and audited break-glass access.
- **Encryption and key sovereignty:** Encryption in transit and at rest; customer-managed keys, BYOK or HYOK; EU-resident HSMs; customer-controlled rotation and revocation; and assurance that the provider cannot silently substitute or recover customer keys.
- **Confidential computing:** Hardware-backed protection for data in use, remote attestation, measured boot and policy-based release of keys only to approved workloads. Requirements should be outcome-based and accept technologies such as Intel TDX, Intel SGX or AMD SEV-SNP where they satisfy the threat model.
- **Open source supply-chain security:** Signed releases and container images, SBOMs, build provenance, dependency governance, vulnerability disclosure, patching SLAs, reproducible or independently verifiable builds, due diligence reports, and documented license compliance.
- **Detection and resilience:** Immutable audit logs exportable to the customer's SIEM, incident-response support, vulnerability management, DDoS protection, immutable backups, tested recovery procedures, defined RPO/RTO values and multi-site resilience.
- **Assurance and auditability:** Independent security audits, penetration-test evidence, contractual audit rights and support for GDPR, and for NIS2 or DORA where the customer's sector is in scope.
- **Exit and portability:** Export of data, metadata, configurations, identities, policies and logs in documented formats; migration assistance; deletion certification; transparent egress costs; and periodic migration testing.

Comparison of the four deployment models

Option	Sovereignty and risk	Services and operations	Portability	Secure enclaves / confidential computing
1. Self-hosted private cloud in	Highest direct control when	Customer assumes responsibility for	Potentially high when based on portable	Technically possible, but the customer must

<p>the customer data center</p>	<p>facilities, administrators, keys and management systems are customer-controlled. External hardware, software and support supply chains still require assessment.</p>	<p>capacity, patching, monitoring, incident response, hardware lifecycle, availability and disaster recovery. Usually the smallest managed-service catalog.</p>	<p>Kubernetes, virtual machines, open APIs and open data stores. Operational tooling and hardware choices can still create lock-in.</p>	<p>procure compatible processors and operate firmware, hypervisor integration, attestation, key release and security updates.</p>
<p>2. Unrestricted public cloud, including international hyperscalers</p>	<p>Sovereignty varies significantly. Data residency may be available, but parent-company jurisdiction, remote administration, telemetry and global subprocessors must be evaluated.</p>	<p>Broadest managed-service, AI, analytics, database, security and global-network capabilities; lowest infrastructure-management burden.</p>	<p>Good at the VM and container layer, but potentially poor when using proprietary databases, serverless services, IAM, messaging or analytics platforms.</p>	<p>Typically the broadest choice, but availability remains restricted to particular regions, instance families and services.</p>
<p>3. International public cloud with EU presence and sovereign controls</p>	<p>Stronger than standard public cloud where the provider offers EU-resident data, keys, control planes, support personnel and administrative boundaries. Residual parent-company and foreign-jurisdiction risk may remain.</p>	<p>Retains much of the hyperscaler catalog, although sovereign regions or offerings may receive fewer services, later feature releases or higher pricing.</p>	<p>The underlying lock-in risks remain unless the architecture deliberately avoids proprietary services and the contract includes an effective exit plan.</p>	<p>Often available in selected EU regions, but must be validated service by service. A confidential VM offering does not mean that managed databases, Kubernetes or AI services use the same protection.</p>
<p>4. EU-owned and EU-operated</p>	<p>Usually the strongest legal and</p>	<p>May offer fewer regions, availability</p>	<p>Can be strong where the provider</p>	

public cloud or hosted solution	operational sovereignty position, provided ownership, personnel, control plane, keys, backups and subprocessors are genuinely EU-bound. Provider nationality alone is insufficient.	zones, managed PaaS services, specialized AI services and marketplace integrations. More engineering may be required to assemble equivalent capabilities.	emphasizes open standards, but EU ownership does not guarantee portability. Proprietary APIs and managed services can still create lock-in.	
--	---	---	---	--

Portability considerations

The EU Data Act has applied since **12 September 2025** and requires cloud and edge providers to facilitate switching and interoperability. It improves the contractual environment, but it does not make applications automatically portable: differences in IAM, networking, database semantics, managed services and operational tooling can still require substantial redesign.

For a genuinely portable solution, require:

- OCI container images and portable Kubernetes, Kata containers or VM deployment.
- Declarative infrastructure-as-code that can target multiple providers.
- Open APIs, open telemetry and commonly supported database protocols.
- Complete export of state, schemas, configurations, access policies and audit history.
- A tested migration procedure and maximum contractual exit period.
- Clear identification of every provider-specific dependency and its replacement approach.

Open source licensing improves inspectability and source-code independence, but **does not by itself ensure cloud portability**. Stateful data services, identity, networking, observability and managed-service dependencies are normally the largest migration constraints.

Impact of excluding international hyperscalers

The principal trade-off is **greater jurisdictional and operational autonomy versus reduced service breadth and convenience**. A pure EU provider may have fewer advanced managed databases, global load-balancing options, integrated security services, serverless platforms, AI accelerators, GPU capacity and confidential-computing instance types. The customer or integrator may consequently assume more responsibility for platform engineering, database operations, observability, scaling and disaster recovery.

Secure-enclave capabilities illustrate this difference. Intel TDX protects an entire confidential VM and generally requires few or no application changes, while SGX provides a smaller application-level trust boundary but normally requires specialized development. Support is tied to specific processor generations, providers and instance families.

Neither technology is a substitute for sovereignty: confidential computing can reduce the cloud operator's ability to inspect workload memory, but it does not independently address metadata, network traffic, control-plane access, availability, foreign legal orders or portability.

For a pure EU end-state, the safest architecture is an open, portable IaaS/Kubernetes and data-services foundation, with proprietary cloud services treated as optional and replaceable. The RFP should evaluate sovereignty by evidence across ownership, operations, keys, support, subprocessors and exit capability - not by provider headquarters alone.